## CLAIMS

1. A method of securing packet data transferred between a group of stations over on a backbone, the backbone comprising an ingress point and egress point, the method comprising the steps of:

receiving, at the ingress point of the backbone, group security association data associated with the group of stations;

receiving a packet at the ingress point of the backbone, a packet including an identifier corresponding to the group of stations and a destination address for the packet;

transforming, at the ingress point of the backbone, the packet according to the group security association associated with the identifier; and

forwarding the transformed packet over the backbone using the group identifier as a backbone address.

2. The method according to claim 1, wherein the step of transforming includes the step of retaining fields of the packet needed to transfer the packet to the destination address over the backbone;

3. The method of claim 1, wherein the ingress point is a customer edge device.

4. The method of claim 1, wherein the ingress point is distributed between a provider edge device and a customer edge device.

5. The method of claim 1, wherein the ingress point is a provider edge device.

6. A method of securing packet data transferred between a group of stations of a private network on a backbone, the backbone comprising an ingress and egress, the method comprising the step of:

receiving, at the egress point of the backbone, group security association data for the group;

receiving a packet at the egress of the backbone, the packet identifying the group and a destination for the packet;

restoring the packet responsive to the the group security association data associated with the group; and

forwarding the packet to the destination.

7. The method of claim 5, wherein the egress point is a customer edge device.

8. The method of claim 5, wherein the egress point is a provider edge device.

9. A method for securely transferring a packet from a source station to a destination station over a backbone, wherein the source station and the destination station are members of a private group, the method comprising the steps of:

registering, by the source station, as a member of the private group including receiving a private group identifier and a group security association;

forwarding, by the source station, a packet to the destination station, the packet including the destination identifier and the private group identifier, the step of forwarding including transforming the packet using the group security association.

10. A network architecture for providing secure communication between at least two members of a private network over a communication link, the network architecture comprising:

a first station;

an ingress point to the communication link;

an egress point from the communication link;

a second station, coupled to the egress point;

a group security association, corresponding to a group of stations in a private network, both the first station and the second station being members of the group;

means for securing data transferred between members of the group from the ingress point and the egress point in the network using the group security association;

means for forwarding the communication between members of the group over the network using a group address associated with the group.

11. The network architecture of claim 10, wherein the communication link comprises a plurality of provider devices, and wherein the ingress point is one of the plurality of provider devices.

12. The network architecture of claim 10, wherein the communication link comprises a plurality of provider devices, and wherein the egress point is one of the plurality of provider devices.

13. The network architecture of claim 10, wherein the group comprises at least three stations.

14. The network architecture of claim 10, wherein the communication link comprises an edge device coupled to a backbone, and wherein the ingress point is the edge device.

15. The network architecture of claim 14, wherein the backbone comprises at least one provider device, and wherein the ingress point is distributed between the edge device and the provider device.

16. The network architecture according to claim 10 wherein the means for securing data includes transform logic for encrypting only a portion of data transferred between the ingress point and egress point of the communication link.